REPORT

2021 年製薬業界の現状と サイバーセキュリティレポート

目次

概要

フォーティネットの「2021 年製薬業界の現状とサイバーセキュリティレポート」では、知的財産、事業継続性、そしてミッションクリティカルなデータの安全確保と保護が遅れ、取り残されつつある業界の現状を明らかにしています。調査した製薬会社の 98% は、少なくとも 1 回は侵入されており、さらに調査した企業のほぼ半数が、昨年の間に 3 回から 5 回もの侵入を経験していました。

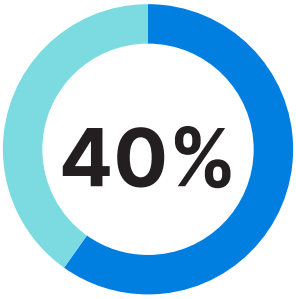
最もよく見られた侵入の手法は以下のとおりです。

40% モバイルセキュリティの侵害

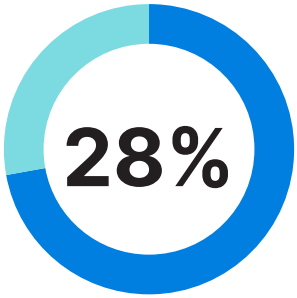
37% フィッシング

36% リムーバブルストレージデバイス / メディアのハッキング

35% SQL、ゼロデイ、中間者（man-in-the-middle）攻撃



の企業が、生産性、安全、コンプライアンス、収益、ブランドイメージなどに影響する操業停止を経験しています。



の企業がビジネスクリティカルなデータまたは知的財産（IP）を窃取されたことがあります。

サイバーセキュリティ対策に最も影響を与えているものは何かという質問に対する製薬業界のリーダーの回答は以下のとおりです。

45% IT と OT の融合

43% 複雑なネットワーク

38% 複雑なサプライチェーン

36% 合併と買収（M&A）

35% 老朽化した OT 環境

35% IoT デバイスの増加

34% 内部の脅威

34% デジタルトランスフォーメーション

一部では、サイバーセキュリティ戦略を改善するために信頼できるパートナーを探している企業もあります。調査に回答した企業がセキュリティプロバイダーに求める能力のトップ 4 は以下のとおりです。

30% 拡張性

25% 革新性

24% 製品のパフォーマンス

21% 可用性 / アップタイム

変化の激しい業界はサイバー犯罪者の格好の標的

製薬業界は、あらゆる面で変化にさらされています。

その一方で、製薬会社は競争に打ち勝つためにますます顧客中心かつデータ中心になってきています。また、多くの企業が以下のような手段で効率を上げようとして、新たなソリューションやソリューションの強化に投資しています。

- デジタルツインを利用してリスクを低減し、資産パフォーマンス管理（APM）をサポートする
- 総合設備効率（OEE）を上げて製造の歩留まりを向上させる
- 定期メンテナンスからコンディションに基づくメンテナンスへ移行して、サービス停止による生産量の低下を最小限に抑える
- 資産の可用性と信頼性を向上させる

一方、サイバー犯罪者はますます洗練され、武装し、企業の IT 環境の隙を付こうとしています。

しかも、製薬会社は他の業界と比べてパートナーエコシステムが複雑で、大学、研究センター、実験室、製造施設、病院などが関わります。したがって、誰もが欲しがる知的財産と患者のプライバシーを守るためには、すべてのつながりをカバーする高度なセキュリティ対策が必要になります。

コネクテッド技術によって拡大するサイバー脅威の対象領域

製薬会社とそこでコネクテッドデジタル技術が使用される状況も、劇的に変化しました。今では多くの製薬会社で情報テクノロジー（IT）システムとオペレーショナルテクノロジー（OT）システムが統合されつつあり、クラウドソリューションを使用したデータ処理とグローバル規模のエコシステムのコラボレーションが広まっています。

しかし多くの場合、これらの変化によってサイバー攻撃の対象領域が拡大しています。以前は大規模なネットワークから隔離されていた OT システムは、今では従来の IT システムと同じネットワークを使用するようになっています。現在、このような OT システムが典型的な IT システム攻撃に対して脆弱な存在となっています。さらに悪いことに、OT システムの攻撃対象領域には IIoT（産業用 IoT）デバイスが含まれていますが、これらの IIoT デバイスは、侵害されると健康や安全に重大な結果をもたらす可能性がある重要システムを制御しています。

さらに、一部の企業はサイバーセキュリティを犠牲にしてオペレーショナルトランスフォーメーションを推進しており、その多くが、システムとデータを守るために必要なエンドツーエンドのスケーラブルなセキュリティ対策を行わないままになっています。

ほとんどの製薬会社では、IT、OT、および物理セキュリティのシステムがそれぞれサイロ化されていますが、それは問題解決の助けにはなりません。データセンター、複数のクラウド、およびエッジの間で IT セキュリティアーキテクチャを統合するだけでも困難を極めます。しかし、攻撃者がサイバー攻撃と物理的攻撃を連携させて同時に仕掛けることができるこの時代には、セキュリティのすべての要素を統合して一元的に可視化することが、唯一の実行可能な保護対策となる場合もあります。

これらすべての要因により、この業界では OT システムが IT ベースの従来の手法を再利用した攻撃や OT に特化したエクスプロイトにさらされるようになっています。製薬業界の重要インフラストラクチャに対する攻撃は、経済的損失、臨床試験の情報漏洩、薬品の汚染、配送の遅延、ブランドの評判低下につながり、ときには生命が失われ、国家の安全が脅かされる可能性さえあります。

この業界の現状と製薬会社が直面しているサイバーセキュリティの課題を本当に理解するために、フォーティネットは「2021 年製薬業界の現状とサイバーセキュリティレポート」の一環として、製薬会社の製造部門の責任者を対象として調査を実施しました。このレポートでは、製薬会社に対する一般的なサイバー攻撃について概説し、企業がサイバーセキュリティソリューションに何を求めているかを明らかにします。

本調査にあたって

この「2021 年製薬業界の現状とサイバーセキュリティレポート」は、2021 年 4 月 15 日～ 19 日に実施された調査に基づいています。調査の目的は、製薬業界の OT のプロフェッショナルが以下について理解を深めるのに役立つ情報を提供することでした。

- 現在の職務の組織内での位置付け
- セキュリティ機能がどのように活用されているか
- 情報がどのように追跡され報告されているか
- 影響と成功要因

以下の条件を満たす回答者から 100 件の完全回答を得るために、パネルサンプルアプローチを使用しました。

- 従業員 501 人以上の製薬、医療機器、またはライフサイエンス分野の企業に所属している
- OT セキュリティとネットワーキングを主要な責任者としてサポートまたは管理している
- サイバーセキュリティおよびネットワーキング関連の購買の意思決定に関与している
- 米国に居住している

製薬業界のセキュリティに関するインサイト：企業がセキュリティソリューションに求めているものとは

前述のように、サイバーセキュリティ態勢の強化または変更に最大の影響を与えるのは、IT / OT の融合とネットワークの複雑さです。最も一般的なセキュリティ対策である社内のセキュリティトレーニングおよび教育、セキュリティオペレーションセンター、ネットワークオペレーションセンター、およびテクニカルオペレーションセンターが配備されている場合、製薬会社のセキュリティの目標は、**リスクの低減（23%）**、**対象範囲の拡大（29%）**、**柔軟性の実現（25%）**、そして**集約品質の改善（23%）**です。

インサイト 1：どの運用機能の評価もきわめて似通っている。

セキュリティソリューションを評価 / 選択するときに以下の運用機能をどの程度考慮するかを重要度の順にランク付けするように求めたところ、有効性 / 効果が最も重要視され、俊敏性と柔軟性が最も軽視されているという結果が出ました。ただし、以下の選択肢の間では、重要度のランクにそれほど大きな差は見られませんでした。

結論：調査の回答者は、理想のサイバーセキュリティツールにすべての運用機能を望んでいます。パッチワークのようなポイントソリューションアプローチではギャップが残ることが多く、すべての機能が欲しいという望みが十分にかなうことはないため、製薬会社にとって最善の選択は、将来も通用するセキュリティ対応を実現できる、ベンダー間の相互運用性とオープンアーキテクチャを備えたエンドツーエンドプラットフォームです。

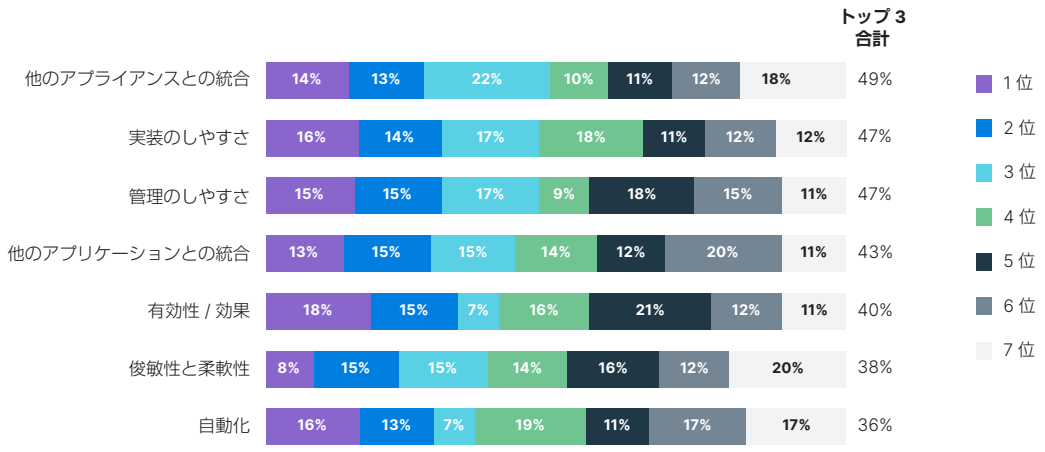


図 1：セキュリティソリューションを選ぶときに考慮する運用機能の重要性ランキング

インサイト 2：生産性機能の重要性はどれもほぼ同等だが、「課題 / 障害の低減」の重要性がやや高い。

時間の節約と課題 / 障害の低減がどちらも 21% でトップの評価を得た一方で、2 番目に望まれる機能としてはセキュリティソリューション全体の透明性が選ばれました。生産性に関するそれ以外の選択肢も後に続いていました。

結論：効率はセキュリティソリューションに不可欠な要素です。製薬会社は、自動オペレーションと人工知能を備えたソリューションを選ぶべきです。これらの機能によって、業務全体で時間とリソースを節約できるだけでなく、人工知能（AI）を活用したインラインの脅威インテリジェンスによってアプリケーション層を保護できます。

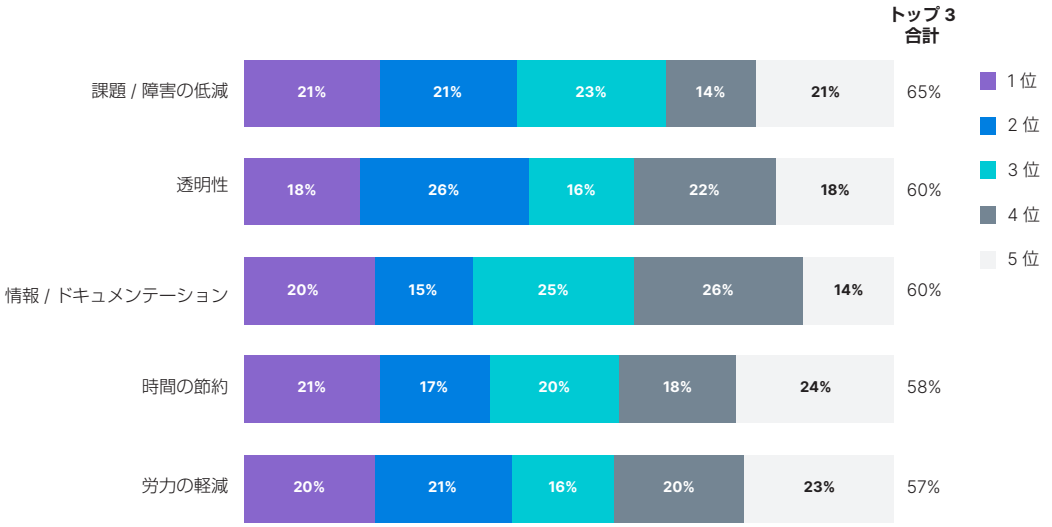


図 2：セキュリティソリューションを選ぶときに考慮する生産性機能の重要性ランキング

インサイト 3：回答者の半数以上が、ソリューションベンダーを選ぶときの優先事項として評判と安定性をトップ 3 に挙げている。

会社の安全に関わるソリューションについては、回答者が評判の高く安定した事業を営むベンダーを好んでいることが明確に示されました。この 2 つの要素は、ベンダー関係をどのように評価するかという質問に対する回答でもリストの上位にあります。

結論：文化的適合と応答性は、セキュリティベンダーを選ぶときにどちらも同程度に重視されますが、包括的ソリューションを提供するベンダーについては、評判が高く、安定した、献身的な（コミットしている）会社が最も信頼されます。製薬会社は市場を評価する際に、セキュリティプロバイダーを慎重に評価するべきであり、プロバイダーの開発件数、保有する特許の数、他のソリューションとの統合件数、そして製品の安定性や市場での高い評判を示す同様の数字を考慮する必要があります。

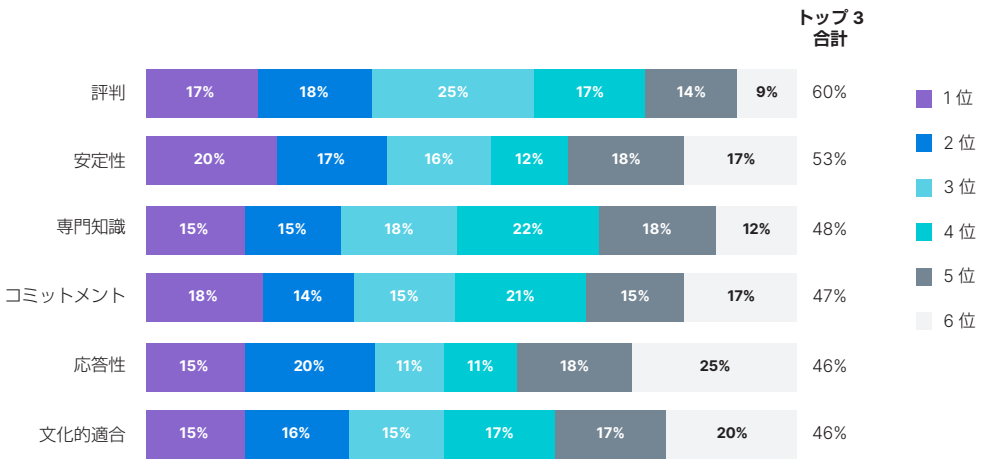


図 3：セキュリティソリューションを選ぶときに考慮するベンダー関係要素の重要性ランキング

インサイト 4：戦略的機能については、集約品質と柔軟性は、リスクの低減や対象範囲ほど重視されていない。

ベンダーを選ぶときに最も重視する戦略的機能として、回答者の 29% が対象範囲を挙げています。また、25% は柔軟性を最優先してソリューションを選ぶと回答しています。

結論:製薬会社が求める対象範囲と柔軟性に優れたソリューションを手に入れるには、コアシステムと統合することができ、調査から試作、製造承認、流通、そして患者の治療に至るまで業務のあらゆるシステムをカバーする、包括的セキュリティを提供するプロバイダーを見つけることが不可欠です。リスクの低減というニーズを満足させるには、製薬会社や他の規制が厳しい業界の組織をサポートした実績のあるセキュリティパートナーを見つけることも重要です。

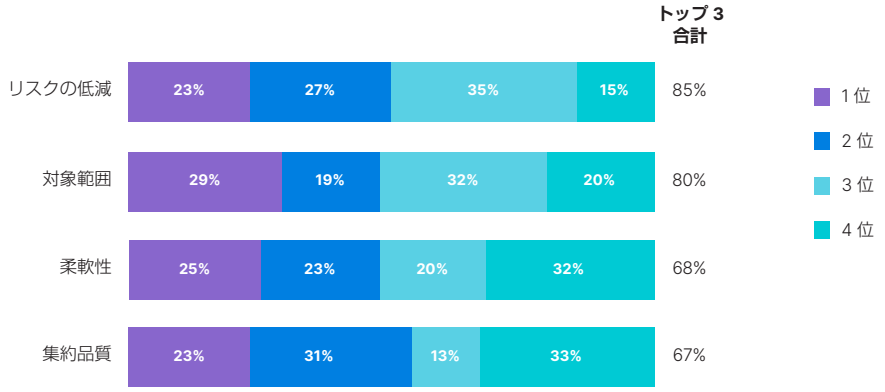
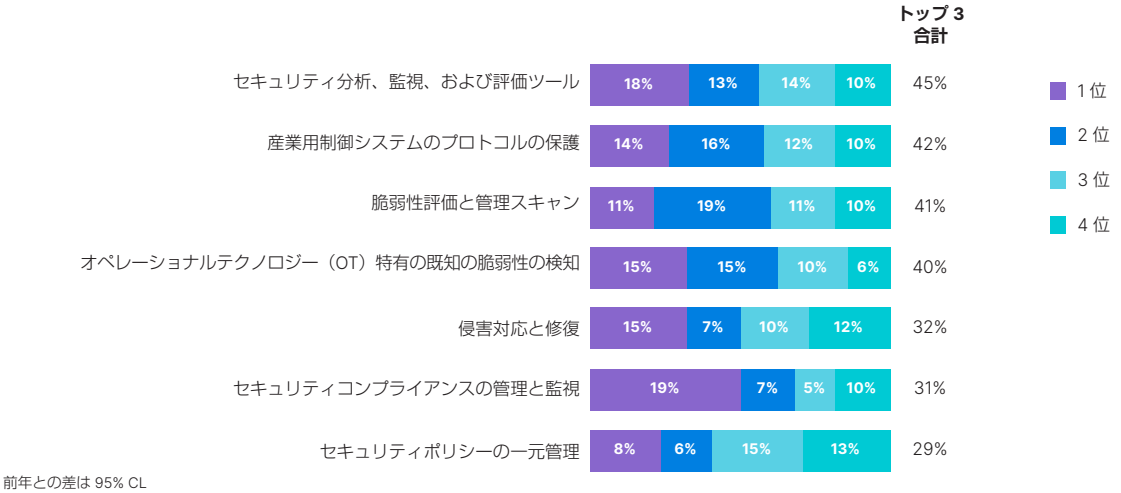


図 4：セキュリティソリューションを選ぶときに考慮する戦略的機能の重要性ランキング

インサイト 5：監視、コンプライアンス、および制御システムプロトコルの保護が、セキュリティソリューションにおける重要度リストのトップを占める。

回答者の 19% にとっては、セキュリティコンプライアンスの管理と監視がセキュリティソリューションの最も重要な機能でした。回答者がその次に重視することが多かったのは、セキュリティ分析、監視、および評価ツールでした。これは、製薬業界のリーダーがプロアクティブな管理に投資し、将来のソリューションについて戦略的に考えていることを示しています。

結論：回答者にとって一部の機能は他の機能より重要ですが、回答がばらついていることは、製薬業界の企業が社内全体のデータを統合できる単一のセキュリティプラットフォームを選ぶべきであることを示しています。それによって、対応のスピードが上がり、IT 部門の負担が減り、経営幹部への効果的な報告が可能になります。セキュリティツールのプラットフォームが複数あると、適切な監視とレポート作成に必要なデータが分断されるだけでなく、IT の複雑さが増し、管理の負担も増えます。



前年との差は 95% CL

図 5：セキュリティソリューションの最も重要な機能（ランキング）

ビジネス上の懸念：トレーニングへのアクセスと変化のペースが最大の障壁

概要

成功を目指すサイバーセキュリティの専門家にとって、以下のことが最も一般的な課題であるという点で、回答者の見解は一致しています。

- 業界の変化に遅れずに対応できる能力
- 法規制の変化
- トレーニングの利用しやすさとアクセス

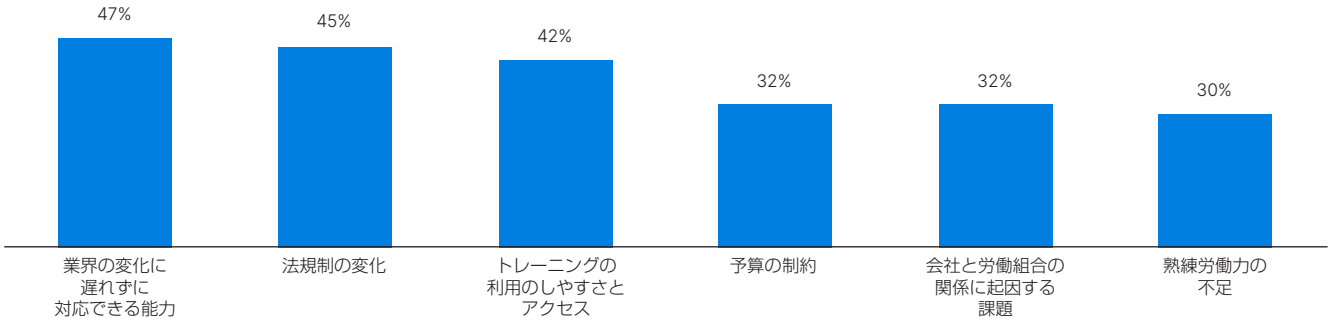


図 6：成功を目指すサイバーセキュリティの専門家が直面する最大の課題（トップ 3）

回答者に、サイバーセキュリティソリューションが OT の専門家の成功に及ぼす悪影響のトップ 3 を挙げてもらいました。最も大きな影響を与えるのは、ビジネス上の懸念と複雑さです。

回答者の 43% はセキュリティソリューションの実装によってビジネス上の懸念が生じると考えており、複雑さが増すと考える回答者が 42%、困難なセキュリティ基準の導入が必要になると考える回答者が 37% いました。これは、サイバーセキュリティに関わる人々にとって、社内での話し合いでセキュリティが利益を生まないコストセンターではなく、成長の要であると見なされるように認識を改めていくことが重要であることを示しています。

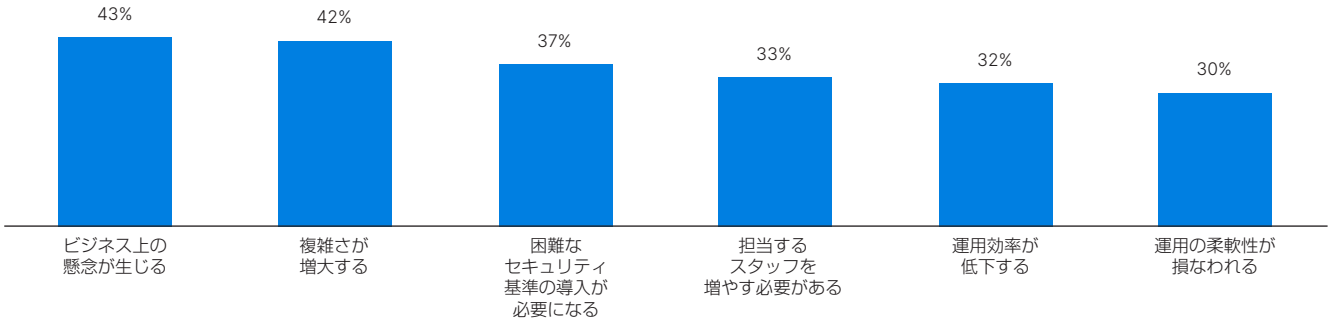


図 7：サイバーセキュリティソリューションは OT 専門家の成功にどのような悪影響を及ぼすか（トップ 3）

企業が受けている侵入の現状とサイバー侵害の影響

製薬会社や医療機器メーカーからバイオテクノロジー企業まで、製薬業界のすべての企業が貴重な機密データを保有しています。特許薬の秘密の化学式、保護された患者の健康情報や顧客情報、そして科学的な研究と進歩は、確実に保護されていない場合、すべてサイバー攻撃の格好の標的となります。

ただし、企業にとって脅威となるのは外部からの攻撃だけではありません。イギリスのサイバーセキュリティ情報保証局（Office of Cyber Security and Information Assurance）によると、製薬業界での知的財産（IP）の窃盗とそれに関連した侵害の 53% は、内部にアクセスできる関係者によって実行されています[1]。また、Health IT Media によると、2018 年から 2020 年までの間に起きた内部関係者による攻撃の 25% は悪質なものであり、人為的なミスや不注意によって引き起こされたものではありませんでした。今回の調査で、医療業界と製薬業界ではこのような内部の脅威によるコストが年間 1,081 万ドルに上っていることがわかりました[2]。

内部からの攻撃は振る舞いも動機もさまざまであるため、内部の脅威から受ける損害は検知も阻止も困難です。たとえば、不満を抱いた従業員が業務を混乱させようとしたり、スタッフが貴重なデータを売ろうと試みたり、善意の同僚がうっかりセキュリティポリシーに違反することさえあり得ます。

今回の調査で、ほとんどの企業が昨年中に少なくとも 1 回は侵入されており、ほぼ半数が 3 回から 5 回の侵入を経験していたことが明らかになりました。また、最も多かった侵入の手口はモバイルセキュリティの侵害でした。

結論：サードパーティベンダーのサイバーセキュリティを継続的に監視するには、ネットワーク全体にわたる完全な可視化と調整が必要です。この問題には、セキュア SD-WAN（ソフトウェア定義型広域ネットワーク）ソリューションによって、WAN エッジ、アクセス層、エンドポイントのすべてにわたってネットワーキングとセキュリティ機能を統合することで対処できます。セキュア SD-WAN ソリューションとセキュア SD ブランチソリューションはこの方法で、急速に拡大と進化を続ける製薬業界のネットワークに対して、高度な可視性、セキュリティ、および保護を実現します。

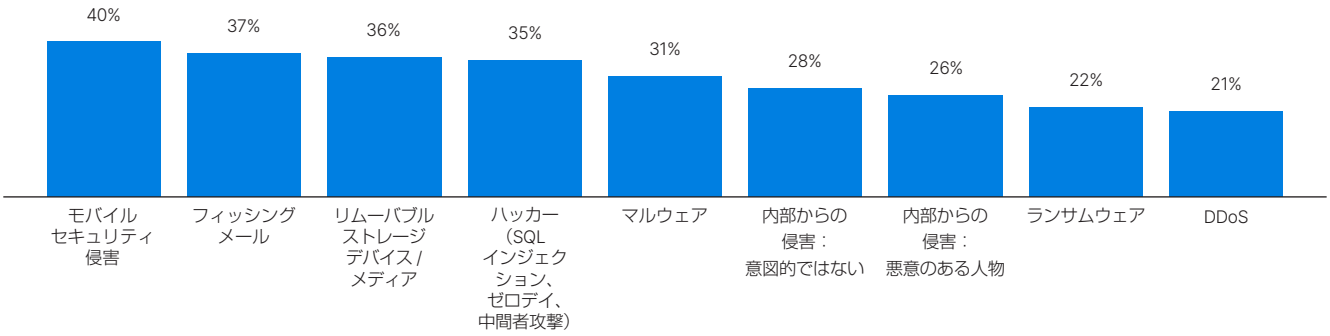


図 8：製薬業界で発生した侵入

侵入はあらゆる分野に同様の影響を及ぼしますが、ビジネスクリティカルなデータ / IP が受ける影響は最小です。

今回の調査に参加した製薬業界のリーダーたちは、サイバー犯罪者によるシステム侵入の阻止に自社がひどく失敗してきたと報告しています。企業にとって最も影響が重大だったのは、生産性に影響し、操業停止を引き起こした侵害で（45%）、それに僅差で続いたのは、身体的安全を危険にさらした操業停止でした（43%）。これらの警戒すべき影響の後に続いたのは、ブランドの評判の失墜（41%）と、収益に影響した操業停止でした。

結論：製薬会社を標的にしたサイバー攻撃は、人命を危険にさらす可能性があります。これだけでも、このような攻撃が起きないようにプロアクティブに防止するべき理由としては十分です。

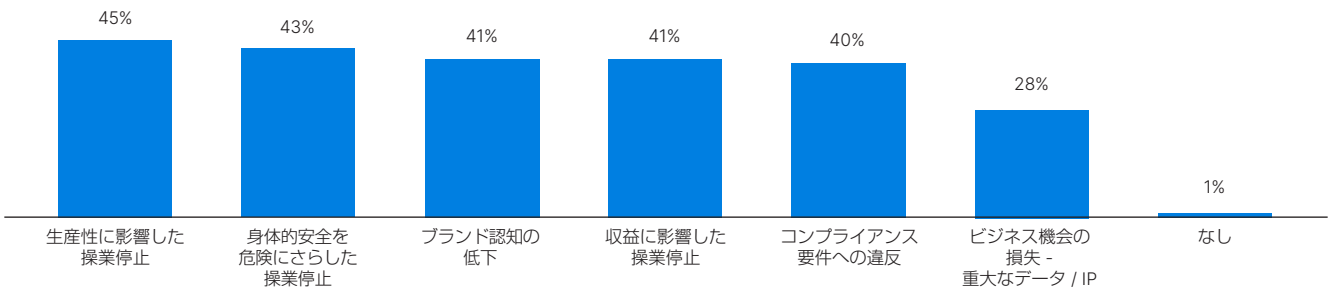


図 9：企業への影響

企業はさまざまな方法でリモートワークを取り入れてきましたが、既存のテクノロジーの採用が最もよく見られた変化でした。

これまでを振り返ると、デジタルイノベーションの取り組みと IoMT（医療分野の IoT）の急速な普及は、製薬会社に脆弱性をもたらしてきました。長年にわたり、クラウドへの移行、コネクテッド医療と遠隔医療、リモートワーカー、そして臨時ワクチン接種会場などによって、製薬業界全体で攻撃ベクトルが増え続けてきましたが、最近ではランサムウェアとフィッシングによる攻撃が突出しています。

結論: リモートワークをサポートするために既存のテクノロジーを採用する必要があったと回答した企業は 30% だけでした。興味深いことに、実装したものを使い続けるのはおよそ 10 社に 1 社だけです。ほとんどの企業は以前のプロセスに戻るか、プロセスを合理化してパンデミック後のコストを削減するための新たな方法を探し続けています。これは、業界の「通常」の操業状態への着実な復帰を示していますが、システムをロールバックするという考えには問題があります。サイバー攻撃がかつてないほど頻繁になり、その損害も増大しているからです。製薬会社は将来を見据えて、パンデミック中の経験から IT 部門とセキュリティ部門が何を学べるかについても考える必要があります。

終わりに：サイバーセキュリティへの最新のアプローチで増大する脅威を迎え撃つ

製薬業界は、ネットワークの複雑さとコンプライアンスの問題から、ランサムウェア攻撃やフィッシング攻撃に対する防御と対応に至るまで、多くのサイバーセキュリティ上の課題と脆弱性に直面し続けています。製薬業界のネットワークは、人の生活を向上させ人命を救うという重要な仕事を続けるために、デジタルイノベーションへの依存を深めていますが、残念なことにサイバーセキュリティの問題もまた増えています。

製薬会社が製薬エコシステムの複雑化とサイバー攻撃の大規模化に対処するには、接続された IT 環境と OT 環境の全体にわたって重要情報の流れを遅らせずに、データを保護できるサイバーセキュリティソリューションが必要です。

フォーティネットは、まさにそのとおりのエンドツーエンドセキュリティプラットフォームを提供する、理想的なセキュリティパートナーです。フォーティネットはあらゆる規模の製薬会社に対応し、接続された IT 環境と OT 環境、そして進化し続ける複雑な製薬エコシステムの全体にわたってデータフローの安全を確保することで、会社の成長を支えます。製薬会社は同時に、デジタル化が進み、顧客中心かつデータ中心の度合いを強めている業務全体の安全を維持できます。

広範で統合されたセキュリティプラットフォームによって、IT 環境と OT 環境の全体にわたって保護を強化し、実用的なセキュリティ対策を施すことができます。フォーティネットは全業務対応の適応型セキュリティ ファブリックによって、エコシステム全体をカバーするセキュリティ、コンプライアンス、および継続的検証の実現に必要な、広範で自動化された統合セキュリティプラットフォームを提供します。

フォーティネットについて、そして成長を続けるお客様の製造エコシステムの保護をフォーティネットがどのように改善できるかについて詳しく知るには、https://www.fortinet.com/solutions/industries/pharma をご覧ください。

参考文献

[1] 「10 Ways Covid-19 Vaccine Supply Chains Need To Be Protected By Cybersecurity」、Louis Columbus、Forbes、2021 年 1 月 24 日（英語）：
https://www.forbes.com/sites/louiscolumbus/2021/01/24/10-ways-covid-19-vaccine-supply-chains-need-to-be-protected-by-cybersecurity/?sh=222b725b26c2

[2] 「Insider Breach Remediation Costs Health, Pharma $10.81M Annually」、Jessica Davis、Health IT Security、2020 年 2 月 6 日（英語）：
https://healthitsecurity.com/news/insider-breach-remediation-costs-health-pharma-10.81m-annually

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

RP-2021-Pharmaceuticals-Cybersecurity-202112-R1